KyberNetwork

A trustless decentralized exchange and payment service

Loi Luu , Yaron Velner
[loiluu, yaron.velner@kyber.network]
(Last updated 21 May, 2017)

Abstract. We design and build KyberNetwork, a new proxy payment system which allows the exchange and conversion of digital assets including crypto tokens (e.g. DigixDao, GolemNetwork Token, Gnosis, Augur, Melon) and cryptocurrencies (e.g. Ether, Bitcoin, ZCash). KyberNetwork will be the first system that implements several ideal operating properties of an exchange including trustless, decentralized execution, instant trade and high liquidity. Besides serving as an exchange, KyberNetwork also aims to provide payment APIs that will allow Ethereum accounts to easily receive payments from any crypto tokens. As an example, any merchant can now use KyberNetwork APIs to allow users to pay in any crypto tokens, but the merchant will receive payments in Ether (ETH) or other preferred tokens.

Although running on the Ethereum network, KyberNetwork's roadmap includes supporting cross-chain trades between different cryptocurrencies using relays and future protocols like Polkadot and Cosmos. Ethereum accounts will be able to safely receive payment from Bitcoin, ZCash and other cryptocurrencies via our payment APIs, through this trustless payment service. Derivatives will be introduced to mitigate the exposure to the risk of volatilities for the users of KyberNetwork Crystals (KNC) and selected cryptocurrencies. This will allow users to participate in the price movements synthetically.

1 Introduction

Emerging cryptocurrencies such as Bitcoin, Ethereum and others have been gaining tractions of late because they allow users to transact, manage their digital assets in a decentralized and trustless model without relying on a third party. More interestingly, Ethereum network, with its turing complete scripting language and trustless smart contracts, makes its easier for people to issue and digitalize their own crypto tokens which either represents some real-world asset (e.g. Digix Gold token) or has values in some platform (GolemNetwork token, Gnosis token, Augur token and so on). To date, the total market capitalization of the most popular cryptocurrency assets is 72 Billion USD[1]. This total market cap has tripled in the last 5 months and is still growing.

[1] https://coinmarketcap.com/charts/

1.1 Motivation

1.1.1 Risk of centralization

As the Blockchain market grows and more crypto assets are being introduced, the need to convert and exchange between crypto tokens is ever increasing. The trade volume between, for example, ETH and Bitcoin is worth hundreds of million of dollars per day on major exchanges. The total trade volume between ETH and other crypto tokens on its network, most of which are less than 2 years-old, is also in the order of millions of dollars. However, despite the decentralized and trustless natures of cryptocurrencies and crypto tokens, most of the trades happening on centralized exchanges are vulnerable to internal fraud and external hacking. This is an ongoing concern and a number of hacking incidents has been reported at various exchanges[2] affecting thousands of users and loss of hundreds of million of dollars.

1.1.2 Lack of instant exchanges

Existing exchanges, including centralized and decentralized ones, often require user to wait for several minutes before allowing them to withdraw their funds.

1.1.3 Existing decentralized exchanges are not working as well as intended

The quests to build decentralized exchanges have been initiated by several parties on the Ethereum network[3]. Although these parties build decentralized and trustless exchanges, they are still vulnerable to external manipulation since there is a delay when an order is created and when it is accepted in a block (read more here).

There are other possible reasons that existing decentralized exchanges are not working as well as intended. These exchanges keep an orderbook of users on the chain. As a result, adjustment or cancellation of bid orders can be expensive. Repeated revisions of orders will compound the issues as the cost will escalate until a match between buy and sell order is found.

One exchange[4] hopes to resolve this issue by making the price discovery and negotiation process done offline via intermediate parties. A trade is done on-chain only after the two parties have agreed on the rate. This raises the issues of trust in the role of the intermediate party in finding the best counterparty for the trade. We also note that no-fees orders are susceptible to adversarial sybil or denial-of-service attacks.

---

[2] For example, MtGox, Bitfinex, Shapeshift.
[3] See 0xProject, OasisIndex and EtherDelta.
[4] Swap.tech

1.1.4 The problem of having many digital assets

As the number of ICOs increases, so does the introduction of new crypto tokens. It is logical to assume that investors will acquire a variety of desired crypto tokens as part of their investment strategy. The convertibility of one crypto token to another represents a new challenge for both investors and operators alike. For example, it may be a challenge for any party to allow an already deployed contract to accept new crypto tokens as a form of payment.

It also introduces more room for implementation bugs and security flaws. As an example, recently, in the DaoToken ICO, there was a major bug that distributed more tokens to SNGLS contributors than to ETH contributors, although they contributed the same amount. Thus, there is a need to simplify the payment procedure for both token holders, merchants and users in the network.

1.2 The KyberNetwork

We introduce KyberNetwork, a proxy payment service providing several useful applications, including building a practical exchange and providing payment APIs for merchants and users to convert tokens effortlessly and "trustlessly". There is no orderbook. Users will know the conversion rate before sending the transaction and receive the corresponding amount. Users don't pay any extra fees (other than the gas fees for the transaction). KyberNetwork benefits through pricing a reasonable spread in the conversion rate.

Our users can also send their existing token A, by converting to a different type of token B and sending it to another user, who only accepts payment in B all in one transaction. More interestingly, KyberNetwork introduces a new standard contract wallet to allow existing contracts, which only accepts few tokens, to receive payments from any future tokens without any modification to the contract code. This allows contracts or merchants to access to a wider class of users, receives payments and contributions in any tokens that KyberNetwork supports.

KyberNetwork's design has several novel constructions to support all these applications.

- Instead of maintaining a global order book, we maintain a reserve warehouse which holds an appropriate amount of crypto tokens for purposes of maintaining exchange liquidity. The reserve is directly controlled by the Kyber contract, and the contract has a conversion rate for each exchange pair of tokens. The rate is frequently updated by the contract owner, i.e. the KyberNetwork operator. When a request to convert from token A to token B arrives, the Kyber contract checks if the correct amount of token A has been credited to the contract, then sends the corresponding amount of token B to the sender's specified address.
- We introduce a new standard contract wallet to enable some of our interesting applications. Specifically, our new standard contract wallet allows the Kyber contract to send a user's newly converted tokens to his/ her destination address on the user's

behalf. The destination address will receive the converted tokens as if the tokens were sent from the sender, not the Kyber contract.

- Our long-term plan also includes employing future features of the EVM language to build an efficient ZCash-Relay on Ethereum. A ZCash-Relay on Ethereum will allow us to support cross-chain trades between ETH and ZEC. We also leverage future platforms like Polkadot and Cosmos to enable more cross-chain trading and payments.
- The Kyber contract is designed with extensibility-focus which has well modularized components. Specifically, we allow dynamically adding any new tokens or delisting existing tokens. Thus, we are able to work with any tokens or digital assets in the future.

2 KyberNetwork's Design

2.1 Actors in the network

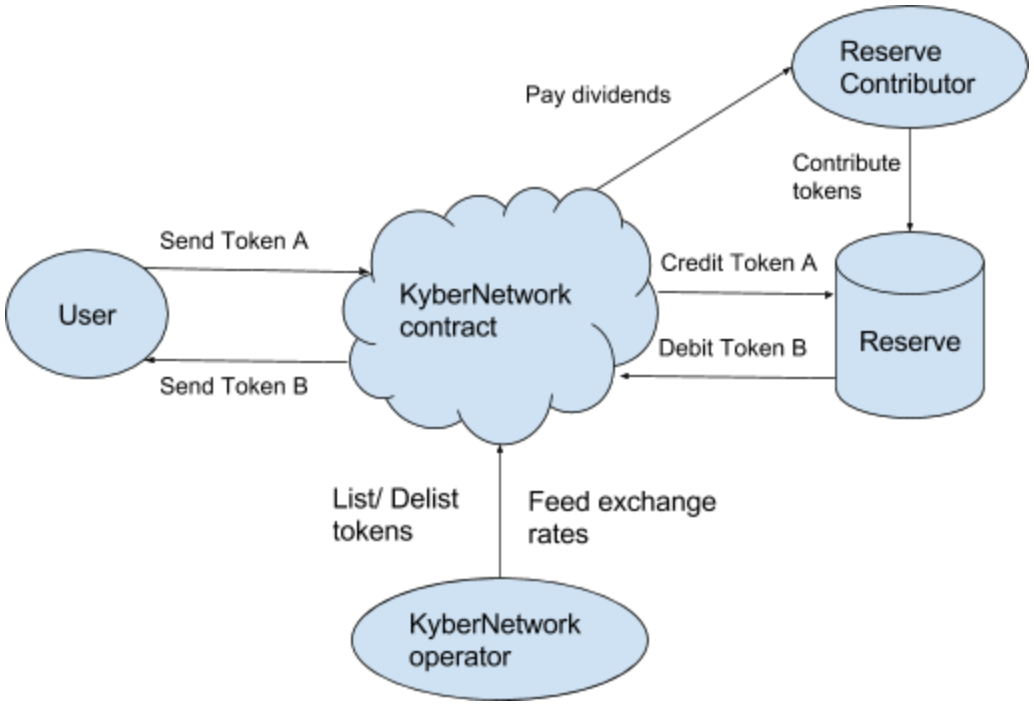
There are 4 roles for the actors in the network:

1. Users who send and receive token[5] to and from the network. Users in KyberNetwork includes individual users, smart contract accounts and merchants.
2. A reserve entity(ies) that provides liquidity to the platform.
3. Reserve contributor who provides capital to the reserve entity and shares the platform profit.
4. KyberNetwork operator who determines exchange rates and feeds the rates to the Kyber contract.

Each of the actors interacts with the smart contract independently in a different way. The users send and receive tokens within a single transaction, without waiting for any response from the reserve or the KyberNetwork operator. The KyberNetwork operator is responsible for determining and feeding the exchange rates to the contract for a fixed period (several seconds basis). The main contract relies on the reserve entity to guarantee high liquidity. The reserve contributor can decide when to contribute to or withdraw from the reserve on their own.

The diagram below illustrates the interaction of each of the actors.

[5] For the rest of this paper a token also refers to the Ether currency.



2.2 KyberNetwork APIs

KyberNetwork supports different API commands for users, reserve and reserve contributors.

2.2.1 User API

User API can be called by any Ethereum account, including normal account and contract ones.

Transfer(amount, source tokens, destination token name, destination address)
Transfer function converts **amount** of source tokens (token A) to destination tokens (token B) and sends type B tokens to destination address. For example, users can call
Transfer(100, "DGD", "Melon", "0xb794f5ea0ba39494ce839613fffba74279579268"*)*
to convert 100 DigixDao tokens to Melonport tokens and transfer all converted Melonport tokens to "0xb794f5ea0ba39494ce839613fffba74279579268".

GetExchangeRate(token A, token B)
Returns the conversion rate between token A and token B. In the future we can support different exchange rates for different trade volumes.

2.2.2 Reserve Contributor API

Reserve Contributor API can only be called by any account in the Ethereum network, though some API only works if the account already contributed.

ContributeReserve(token type, amount)
Contribute some amount of tokens of a certain token type to the reserve. For every contribution, the contributor will receive some amount of KyberNetwork Crystals (KNC) to represent their contribution to the platform.

WithdrawDividends()
Dividends are distributed proportionally to the contributions of the contributors. The exact formula to distribute the platform profits will be available in the next version of the paper.

WithdrawContribution(KNC amount, token type)
An existing contributor can withdraw their contribution by burning some KNC tokens. The contributor can specify in which token type that he wishes to receive for his withdrawn contribution.

2.2.3 Operator API

ListPair (token A, token B, initial rate)
To introduce a new pair of tokens that KyberNetwork supports.

DelistPair (token A, token B)
To stop accepting trade between a pair of tokens.

SetRate(token A , token B, rate)
To set a conversion rate between an existing pair of token A and token B. In the real deployment, this API will be replaced by a different API which updates the rates of all existing pairs in one transaction. The purpose of batch-update is mainly to reduce the gas cost.

2.3 Support trustless trading cross-chain

Chain relays, e.g. BTCRlay, enables communication between different blockchains. The launches of protocols like Polkadot and Cosmos will make cross-chain interactions even easier. KyberNetwork will leverage these technologies to allow Ethereum accounts to receive payments from different cryptocurrencies.

3 System Properties

3.1 Trustless and secure

The KyberNetwork operator does not hold the tokens of the users. Hence, by design, user's tokens are secured from theft losses. Users need not trust the intentions of the reserve entity and the KNC token holders, as the integrity of the operator is enforced/ensured by the smart contract.

3.2 Instant trade

An exchange or convert request is executed immediately within a single transaction. Users get their exchanged token at the exact moment they transferred their original token. No deposit or confirmation or waiting time is needed. Providing this efficient and user friendly feature differs KyberNetwork from most existing and future exchanges.

3.3 On-chain exchange

The exchange runs on chain and is accessible for all accounts, including normal accounts and smart contracts. That allows smart contracts to directly interact with the exchange without a third party intervention to receive funds/ payments from different tokens that they do not support originally. This feature enables us to be an on-chain proxy payment platform for all accounts, including normal accounts and smart contracts.

3.4 Compatibility

KyberNetwork does not require any changes in the underlying protocol of Ethereum and existing smart contracts. Our payment API can communicate with existing contracts without any change on their side.
That said, we also introduce a new contract wallet that holds all user Ether and tokens. The wallet allows the user to pay with token A to a contract that expects token B, where the conversion from A to B is seamlessly done by the KyberNetwork. The receiver will receive the payment as if it was sent by the original user.

3.5 Alignment of interests

The KyberNetwork operator serves the interests of the KNC token holders. It is the interest of both to serve the interest of the users, attract more users and also increase the trade volume.

3.6 Comparison to existing systems

We compare KyberNetwork to existing systems in the table below.

Exchange	Trading Cost[6]	Trustless	Instant Trades	On-chain	Liquidity	Secure against attacks
Kraken/Poloniex	Low	No	No	No	High	No
Shapeshift	Low	No	Yes	No	High	No
Coinbase	Low	No	Yes	No	High	No
EtherDelta 0xProject Oasis Index	High	Yes	No	Yes	Low	Yes
Swap.tech	Low	Yes	No	Hybrid	Low	Not sure
KyberNetwork	Low	Yes	Yes	Yes	High	Yes

4 Applications

4.1 Instant and secure exchange

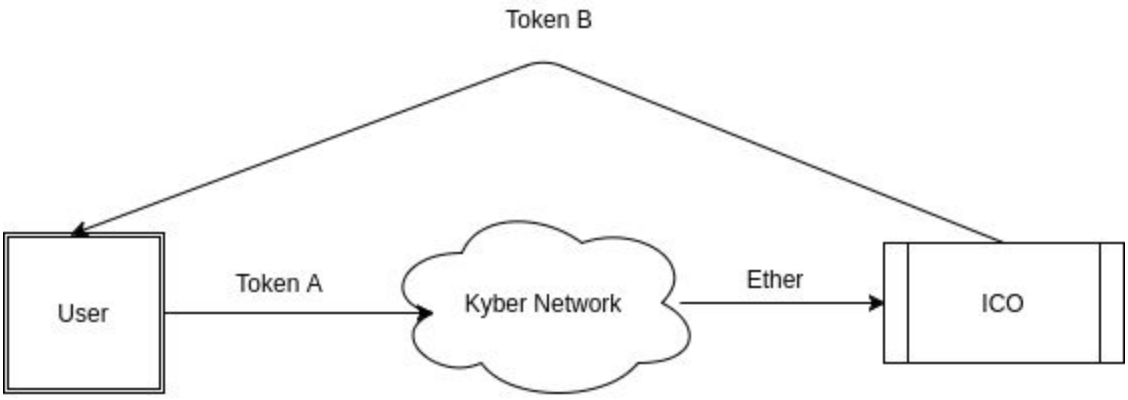
First and foremost, KyberNetwork is an exchange. Unlike most exchanges, however, KyberNetwork performs trade requests instantly. Moreover, KyberNetwork does not hold users' tokens, thus any theft or loss of tokens is prevented by design.

This is in sharp contrast to most exchanges where confirmation time of several minutes is typically needed. Any malfunction during that period could potentially result in inconvenience or in the worst case scenario, loss of funds.

4.2 Generic payment APIs with any token

Conducting an exchange over a smart contract allows user to pay for any service or product with any crypto token they prefer. The contract will provide instant conversion to Ether and securely pay on behalf of the user to any contract he wishes. The figure below describes how a user could participate in an ICO that accepts only Ether with any token. The entire process occurs within a single transaction, and the KyberNetwork never has a possession on the user tokens (neither token A nor token B).

[6] Cost to execute a trade, apart from the trading fees.



4.3 Trusted on-chain source for rate quotes

KyberNetwork exchange rates are visible to other smart contracts. Hence, it enables the implementation of advanced financial instruments such as swap contracts. The quotes provided by KyberNetwork are secure as they reflect the real rates which are being used to trade between pairs of tokens.

4.4 Mitigate the risks of price fluctuations

Due to the illiquidity of crypto assets, the exchange rates often seem too volatile due to irregular demand and supply. This issue is aggravated further due to lack of parties that are willing to warehouse. It is almost impossible now for users of crypto assets to hedge themselves for future requirements. The KyberNetwork will be addressing this challenge by introducing derivatives in the forms of forwards and options to provide more alternatives to users.

4.5 Forwards

A forward is a contract whereby parties agree to trade an asset at a later date at a price specified in the present. One of the common problems as ICOs become mainstream is the need for some users to convert between tokens, such as from Melon to ETH, in preparation to participate in an upcoming ICO. The user could either acquire ETH at current market rate or commit to a forward contract to negate the risk of the price fluctuations in the ETH as an viable alternative.

4.6 Options

Options contracts allow users to hedge against adverse price movement for a fee called premium. A call option gives the owner of the contract the right to purchase the crypto asset at an agreed price. A put option is an opposite. The premium is calculated using the implied volatility of the underlying crypto asset.

The user of crypto assets that need to prepare for a future purchase or sale commitments can pay a premium to buy a call or put option. As an example, holders of iced tokens are able to write call options to earn premiums while forgoing the upside of the price.

5 Road map

The road map of KyberNetwork includes several phases.

- Phase 1: Support trading and proxy payments between any tokens to and from Ether.
- Phase 2: Support trading and proxy payments between arbitrary token pairs.
- Phase 3: Support trading advanced financial instruments.
- Phase 4: Support cross-chain trading. Users can trade between Ether/ tokens to Bitcoin, ZCash, ETC and so on.

The details of each phase will be available in the next version of the paper.

6 Acknowledgement

We thank our advisors, namely Wong Lee Hong, Vitalik Buterin, Leng Hoe Lon, Prateek Saxena and our friends, namely Stelian Balta, Reto Trinkler for their feedback on the earlier version of this paper.

7 The team

7.1 Core members

1. **Loi Luu**
   Loi Luu is a researcher working on cryptocurrencies, smart contract security and distributed consensus algorithms. His research publications are available online, and he is a regular invited speaker at Bitcoin and Ethereum workshops such as DevCon2, EdCon, Scaling Bitcoin.
   Loi believes in the force of the Ethereum and Blockchain technology. Much of his work revolves around this community. He developed Oyente, the first open-source security analyzer for Ethereum smart contracts. Next, he cofounded SmartPool, another open source project which embraces decentralization of mining pools in existing cryptocurrency. He continues to champion decentralisation and trustless properties of the Blockchain with KyberNetwork, taking inspiration and developing value for the community.

2. **Yaron Velner**
   Yaron Velner is a researcher and a co-founder of the SmartPool project. His research is focused on aspects of game theory incentives in blockchain protocols and formal

verification of smart contracts. He holds a Phd in computer science from Tel Aviv University. In his Phd thesis he investigated applications of game theory techniques to formal verification of computer programs and systems.
Yaron is also an experienced software developer with over 10 years of experience as a senior software engineer and a technical leader at EZchip semi-conductors (recently acquired by Mellanox technologies). At EZchip he was a member in the data structure and algorithm team, which developed novel data structures for IP routing.

3. **Victor Tran**
   Victor Tran is a senior backend engineer and Linux system administrator. He has experience in developing and building infrastructure for multiple social marketing platforms and advertising networks. He is interested in building high performance multi-platform applications.
   Victor co-founded and was CTO of several startups in social marketing. He built and maintained platforms which handled millions of monthly active users. Victor is currently the lead engineer in the SmartPool project.

4. **Cuong Nguyen**
   Cuong is a senior web developer with several years building interesting web applications. He recently spends most of his time on playing around with various blockchain platforms including Bitcoin, Ethereum and IBM's Fabric ledger.

7.2 Advisors

1. **Wong Lee Hong**
   Wong Lee Hong career spans across various industries over 3 decades. He has extensive distribution and business development experience in consumer electronic, multimedia, computer gaming, internet and the banking sectors. The second half of his career was spent developing the Internet Banking capability of a major financial institution, venture capital activities in strategic startups and regulatory management role, dealing with banking regulators in Asia in matters relating to banking technology and operations. At present, he is a Blockchain enthusiast and investor.

2. **Leng Hoe Lon**
   Leng Hoe Lon co-founded Shentilium with National University of Singapore, with the aim of using the latest data-driven technology to drive business decisions and gain competitive edge. He also co-founded TrackRecord Asia, with the vision that anyone can learn to trade in the financial markets profitably within a professional risk management framework. Prior to this, he held various positions in the financial industry including Deustsche Bank (London and Singapore), JPMorgan (Singapore), ABN Amro (Singapore). He was a Managing Director in Goldman Sachs' Asia Macro Trading group

in HK and Asian FX trader in London. He was also CEO of Tudor Capital Singapore, a global macro hedge fund.

3. **Prateek Saxena**
   Prateek Saxena is a research professor in computer science at National University of Singapore. He works on blockchains and computer security. His research has influenced the design of browser platforms, web standards and app stores widely used today. He has received several premier awards such as the MIT TR35 Asia.

4. **Vitalik Buterin**
   Vitalik is the Founder and Chief Scientist of Ethereum. He is also both the Founder and a writer for Bitcoin Magazine, a venture that marked the beginning of his career in crypto in 2011. He is interested in creating secure, efficient, and trustworthy systems and advises a number of projects in the crypto space.